Architectural Reference Working Group

Meeting Minutes

29 October 2020

Attendees: Adam Montville, Mitch Thomas, Russ Warren,
Forrest Hare, Duncan Sparrell, Doug Austin, David Kemp, Stephen Wood,

Agenda: Completing a 'version 1' of our architecture by the end of this year.

We took several actions from our last call:

- We should focus on a couple of workflows, as examples. Adam has offered to share the workflows (CIS 7.1 controls) as a starting example.
- It was suggested we look at the C4 Model (c4model.com) as a way to document(visualize) the architecture diagram.
- Make our current diagram a functional architecture (eliminate products) and update to the latest SCAP level were identified as good next step for our diagram. JK has volunteered to do these updates. We will also need to create a terminology/reference document. JK will also create a working version of a glossary.

Adam reviewed the CIS Controls v7.1 diagram. Adam discussed workflows and procedures that would use multiple people/systems. Adam is suggesting the controls show the tools and the relationships between them but not about interaction or workflows. How do the management categories interact with each other? We want to show how the interaction among the management categories. Doug Austin mentioned cyberscape reports? Version 2.9 file has 19 categories (cyber-service areas) and 100s of vendors. CDM (cyber-defense matrix) is another reference we can look at.

Adam reviewed the diagrams next. He wants to tie to SCAP. He applied C4 to the posture assessment system (SCAP system). Context, Container, Component diagrams were provided. Adam walked through the diagrams. Query/Response aspect (Mitch); create a flow of events (input and output). Open DXL can stream the information. We should include the human element in our diagrams (at the context level). We should show who is using the information and what they are trying to achieve. SCAP is on sense making part, not decision making and acting part of the overall architecture. SCAP application uses posture collection service. We need to define what the posture assessment system output is. We need to continue to evolve (ex. Firewall). We need to use cases and description of what is on the charts.

At the highest level, start with a use case. C4 model lines (dependency or flow) and directionality? Security posture of the endpoint is a key use case. What data do we need to collect (threat, vulnerabilities, endpoint information)? Should we identify these first? And what needs it?

Turn our architecture into a context diagram. No more than 5-6 use cases could be used for a diagram. Endpoint, firewall and vulnerability scope? Doug can help with use cases.

Chat content:

from Duncan Sparrell (External) to Everyone: 4:41 PM

what am I doing wrong?
https://github.com/opencybersecurityalliance/documentation/tree/master/architecture looks empty to me. Is there a branch strategy (I see there are two branches besides master) and what is it? I suggest the master readme have something about whatever the branch strategy is so we can find anything.

from Douglas Austin (External) to Everyone: 4:50 PM

Here is Momemtum Cyber's 2020 version of the CYBERscape - as was mentioned, this graphic is used to show "just how big" cyber vendor space is... it's quite an eye chart:
https://momentumcyber.com/docs/CYBERscape.pdf

from Douglas Austin (External) to Everyone: 4:50 PM

*Momentum

from Douglas Austin (External) to Everyone: 4:51 PM

I don't see a copyright on it.

from Duncan Sparrell (External) to Everyone: 4:52 PM

https://owasp.org/www-project-cyber-defense-matrix/ is also worth looking at if you want to make sure you are covering all dimensions. It is a 5x5x5. Threre are several RSA talks on it which shows gaps

from Mitch Thomas (External) to Everyone: 5:12 PM

+1 for using these pictures!

from Duncan Sparrell (External) to Everyone: 5:22 PM

Apologies but I need to drop

from Douglas Austin (External) to Everyone: 5:24 PM

endpoint, firewall, vuln scan?